WEB BASED SYSTEM FOR MICROSOFT ACTIVE DIRECTORY REPORTING AND EVENT CORRELATION USING DATA MINING

M.S.P. Perera

This dissertation was submitted in requirements for the Master of Engineering degree Master of Science in computer science

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

December 2008

93368

Abstract

Microsoft Active Directory is very popular in large and medium scale organizations as a system for centralized management of users, desktops, servers, printers and mail boxes etc. This provides a centralized console for managing and viewing the objects very easily. The Active Directory data repository could be used to generate many management reports that would be useful for taking future management decisions and analyzing the health of the organization's security. Many events are generated as a result of user activities and status changes of the objects. These events are reflected on the active directories and event logs. The correlation and outlier analysis of the events is important to filter out thousands of non critical events and be pro-active on important critical events.

This thesis discusses generating management reports, by querying the Active Directory database and providing real time alerts to system administrators on critical events, with the use of data mining techniques such as event correlation and outlier analysis.

The scope of the event analysis is limited to data generated in the Microsoft Active Directory.

Keywords: Microsoft Active Directory, MS AD, Event Correlation, AD Reports, Outlier Analysis, Event Log Clustering.